UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/693,713	10/19/2000	Kunihiko Miyazaki	16869P-011500	7398

20350 7590 01/04/2005

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 01/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/693,713	MIYAZAKI ET AL.	
	Examin r	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspond nce address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 September 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-7,9-14,16-21,23-30 and 34-37* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-7,9-14,16-21,23-30 and 34-37* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 September 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 2, 4-7, 9-14, 16-21, 23-30, and 34-37 are pending in this office action, claims 34-37 are newly added.

2. Applicant's arguments filed September 13, 2004, have been fully considered but they are not persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

4. Claims 1, 2, 4-6, 13, 14, 16-20, 27-29, 34, and 36 are rejected under 35 U.S.C. 102(a) as being anticipated by Schneier et al. (U.S. Patent No. 5,956,404).

Regarding claims 1, 13, and 27, Schneier et al. teaches a digital signing method/apparatus/computer program, comprising:

- A processor (col. 5, lines 22-28); and
- A storage medium (col. 5, lines 28-35);
- Wherein said processor applies a secret key to a message to generate a digital signature for the message (col. 5, lines 7-15);

- Wherein said processor registers log data **comprising the digital signature and the message** with a log list in said storage medium (col. 11, lines 30-42); and
- **Wherein said processor further applies the secret key to the message and to computed data to generate the digital signature, the computed data being determined based on a previously generated digital signature and on a previous message that are retrieved from the log list** (col. 6, line 65 through col. 7, line 15 and col. 11, lines 30-64)**; and**
- **Wherein said processor distributes the computed data along with the generated digital signature and the message** (col. 10, lines 34-37)**.**

Regarding claim 28, Schneier et al. teaches wherein the computer readable storage medium is a computer readable medium for storing the codes (col. 5, line 26).

Regarding claim 29, Schneier et al. teaches wherein the computer readable storage medium is a computer readable medium for transmitting the codes (col. 5, line 26).

Regarding claims 2 and 14, Schneier et al. teaches wherein said message is a hash value of another message (col. 6, line 65 through col. 7, line 15).

Regarding claims 4 and 16, Schneier et al. teaches wherein:

- Said log data further comprises a distribution destination (col. 6, lines 27-29), and

- Wherein said log data including a distribution destination attached thereto (col. 11, lines 30-42).

Regarding claims 5 and 17, Schneier et al. teaches wherein registration of the log data with said log list is permitted only when the data from a previously signed message is included in the latest log data registered with said log list (col. 11, lines 45-48).

Regarding claims 6 and 18, Schneier et al. teaches

- Wherein said processor obtains a timestamp from a trusted authority, said timestamp generated by applying a second secret key to the digital signature, and a time (col. 12, lines 41-48); and
- Said processor **further distributes** the timestamp, **along with the generated digital signature, the computed data,** and the message (col. 12, lines 45-47 and fig. 3, ref. num 285).

Regarding claim 19, Schneier et al. teaches further comprising an interface configured to be connectable to a computer (col. 5, lines 24-28).

Regarding claim 20, Schneier et al. teaches:

- Wherein if a number of the log data registered with the log list exceeds a particular value, said processor outputs at least one of a plurality of log data

registered with the log list to said computer, whereupon said computer registers said at least one of a plurality of log data with a second log list prepared in said computer (col. 11, lines 5-13), and thereupon,

- Said processor deletes said at least one of a plurality of log data from said log list in said storage medium (col. 11, lines 13-15).

Regarding claims 34 and 36, Schneier et al. teaches wherein the registering further includes registering the computed data (col. 11, lines 25-27).

Claim Rejections - 35 USC § 103

5. Claims 7, 9-12, 21, 23-26, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier et al. (U.S. Patent No. 5,978,475), hereinafter referred to as '475, in view of Schneier et al. (U.S. Patent No. 5,956,404), hereinafter referred to as '404.

Regarding claims 7, 21, and 30, '475 teaches a digital signature verifying method/apparatus/computer program, comprising:

- A processor interconnected with an input device (fig. 1B, ref. num 110 to 180);
- Accepting a message (col. 13, lines 15-16);
- Acquiring a log list of a digital signer (col. 13, lines 17-22); and
- Checking whether log data of said digital-signature-attached message is registered in said log list (col. 13, lines 23-33),

- And if the log data is registered in the log list, authenticating that the digital-signature-attached message was distributed by the digital signer (col. 13, line 65 through col. 14, line 1),
- **Wherein said processor authenticates whether the digital signature included in said digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer** (col. 15, lines 1-8)**.**

'475 does not specifically teach the accepting is of a digital-signature-attached message, wherein said digital-signature-attached message may have been distributed by said digital signer is to be verified.

'404 teaches accepting a digital-signature-attached message (col. 5, lines 35-41), wherein said digital-signature-attached message may have been distributed by said digital signer is to be verified (col. 11, lines 45-48).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine accepting a digital-signature-attached message, wherein said digital-signature-attached message may have been distributed by said digital signer is to be verified, as taught by '404, with the method/apparatus/computer

program of '475. It would have been obvious for such modifications because a digital-signature-attached message provides a strong audit trail; a strong audit trail provides an indisputable list of actions to verify all events that took place.

Regarding claims 9 and 23, the combination of '475 in view of '404 teaches:

- Wherein said digital-signature-attached message further comprises data from a previously signed message (see col. 11, lines 30-64 of '404),
- Said method further comprising checking whether the digital signature included in the digital-signature-attached message has been generated for the message included in the digital-signature-attached message, using the digital signature, the data from a previously signed message, and the message included in said digital-signature-attached message and a public key paired with a secret key of said digital signer (see col. 15, lines 12-15 of '475).

Regarding claims 10 and 24, the combination of '475 in view of '404 teaches said method further comprising checking whether data from a previously signed message included in said digital-signature-attached message is included in the log data registered immediately before log data of said digital-signature-attached message in said log list, and if the data from a previously signed message is included in the immediately previous registered log data, authenticating that said log list has not been altered (see col. 11, lines 45-48 of '404).

Regarding claims 11 and 25, the combination of '475 in view of '404 teaches:

- Wherein said log data further comprises a distribution destination (see col. 6, lines 27-29 of '404),
- Said method further comprising acquiring a digital-signature-attached message from the distribution destination attached to the log data registered immediately before/after the log data of said digital-signature-attached message in said log list (see col. 11, lines 30-42 of '404), and
- Checking whether the acquired message is included in said immediately previous/subsequent registered log data, and if the message is included, authenticating that said log list has not been altered (see col. 11, lines 44-50 of '404).

Regarding claims 12 and 26, the combination of '475 in view of '404 teaches:

- Wherein said digital-signature-attached message further comprises a timestamp created using a second secret key (see col. 12, lines 41-48 of '404),
- Said method further comprising acquiring a digital signature and a time data by applying a public key paired with said second secret key to the timestamp included in said digital-signature-attached message (see col. 12, line 65 through col. 13, line 1 of '404); and
- Checking whether date and time indicated by the acquired time data exceeds a date and time of signing of said digital-signature-attached message (see col. 12, lines 49-59 of '404),

- And if the date and time indicated by the time data does not exceed the date and time of signing of said digital-signature-attached message, authenticating the validity of the acquired digital signature (see col. 12, line 59-65 of '404).

Regarding claims 35 and 37, the combination of '475 in view of '404 teaches wherein the digital-signature-attached message that is registered in the log list includes data based on a previously generated digital signature and on a previous message (see col. 6, line 65 through col. 7, line 15 of '404).

Conclusion

6. Applicant amends claims 1, 4, 5, 7, 13, 16-18, 21, 27, and 30, and cancels claims 3, 8, 15, 22, and 31-33.

7. Applicant argues Schneier et al. does not contain signature data as claimed in the instant application because Schneier et al. appends chain data before generating a signature (page 17, third paragraph). Also, Schneier et al. does not show how to verify the audit trail using previous signatures (page 17, last paragraph).

Regarding applicant's argument, examiner disagrees with applicant. Applicant is referred to column 7, lines 7-15 and figure 5. This shows that even though only the most prior signed signature is stored, ANY prior signed signature can be found by tracing back through the previous signatures. Therefore, any of the previous signatures can be verified, not just the most prior one. The data is shown as being appended

before the generation of the signature; however, the appended data has already been signed in previous signatures. The new signature now appends the previous signatures to include them into the new signature. This creates a chain of signatures that prevent an attacker from altering any previous signatures.

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brenda Hall

BH

EMMANUEL L. MOISE
PRIMARY EXAMINER